Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

Datum:	4. Januar 2022
Version:	v1.0
Autor:	NCSC/GovCERT.ch
Kontakt:	outreach@govcert.ch
Verteiler:	Gesundheitssektor MELANI, H+, HIN, BAG, Swissmedic

Aktuelles (Dezember)

Die Risikoexposition im Bereich Cyber für das Gesundheitswesen bleibt weiterhin hoch. Akteure nutzten die Ferienzeit zwischen Weihnachten und Neujahr aus, um Cyberangriffe gegen Organisationen zu fahren. Dies im Hinblick darauf, dass sich viele IT-Spezialisten in den Ferien befinden und ein Cyber-Angriff auf das Unternehmens-Netzwerk möglicherweise zu spät entdeckt wird.

Das aktuelle Healthcare Update behandelt folgende Themen:

- Kritische Verwundbarkeit in Java-Bibliothek «Log4j»
- Ransomware Angriff auf Gesundheitswesen
- In eigener Sache

Kritische Verwundbarkeit in Java-Bibliothek «Log4j»

Anfangs Dezember wurde eine kritische Verwundbarkeit in der weit verbreiteten Java-Bibliothek «Log4j» bekannt[1], welche es einem Angreifer ermöglicht, aus der Ferne beliebigen Code auszuführen («Remote Code Execution» - RCE). Kurz nach bekannt werden der Sicherheitslücke wurde diese bereits breitflächig von Cyberkriminellen ausgenutzt, um Organisationen zu kompromittieren. Das NCSC hat im Monat Dezember hunderte solcher Angriffe festgestellt und kurz nach bekannt werden der Sicherheitslücke bereits Gegenmassnahmen eingeleitet, um Organisationen mit verwundbarer Software in der Schweiz zu schützen. Zusätzlich hat das NCSC Dutzende Organisationen in der Schweiz informiert, welche potenziell verwundbare Software im Einsatz haben. Bislang haben Akteure vor allem Linux Malware («Mirai», «Kinsing» und «Tsunami») aber auch Windows Malware («Dridex» und «CoinMiner») über die Sicherheitslücke verteilt.

[1] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/log4j.html

Dem NCSC sind auch Fälle von Angriffen auf «Log4j» bekannt, in welchen Angreifer das Netzwerk des Opfers mit Ransomware verschlüsselt haben[2]. Auch das belgische Verteidigungsministerium wurde kürzlich Opfer[3] eines Angriffs auf «Log4j», wobei die genauen Absichten der Täterschaft vorerst nicht bekannt waren.

Log4j ist in vielen Drittprodukten im Einsatz. Folge dessen sind viele Produkte und Open-Source Software von der Verwundbarkeit betroffen. Das NCSC empfiehlt daher, sicher zu stellen, dass sämtliche Software stets auf dem aktuellsten Patch-Level gehalten werden. Es ist wichtig, dass dabei nicht nur die eigentliche Software, sondern ebenfalls alle Abhängigkeiten (Dependencies) dieser Software im Auge behalten werden und dass die Verantwortlichkeit für deren Pflege klar geregelt ist.

Weitere Informationen zur Verwundbarkeit in «Log4j» finden sich auf der Webseite des NCSC und GovCERT.ch.

Kritische Sicherheitslücke in Java-Bibliothek «Log4j»:
https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/log4j.html

Zero-Day Exploit Targeting Popular Java Library Log4j:
https://govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/

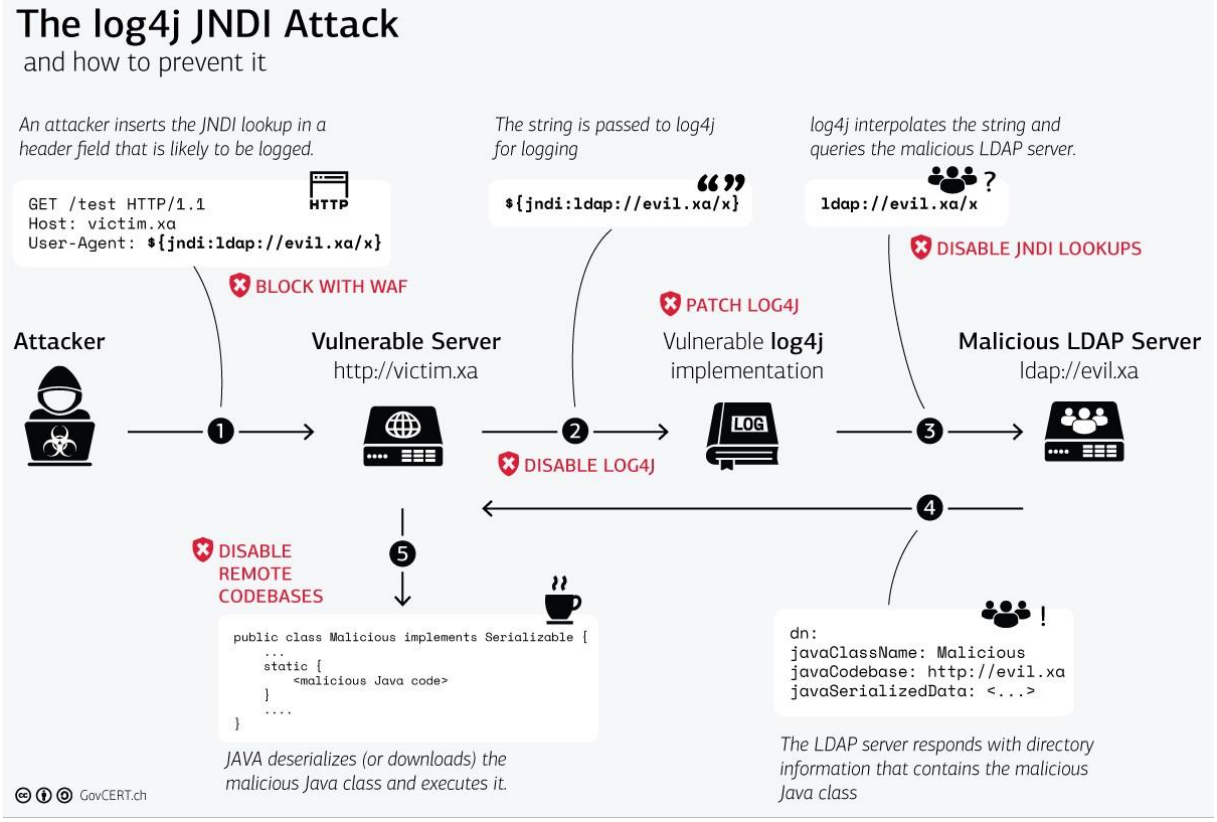

Figure 1 - Ablauf eines Angriffes auf "Log4j"

[2] https://www.zdnet.com/article/conti-ransomware-attacking-vmware-vcenter-servers-through-log4j-vulnerability/$

[3] https://www.cyberscoop.com/intruders-leverage-log4j-flaw-to-breach-belgian-defense-department/

Ransomware Angriff auf Gesundheitswesen

Auch im Monat Dezember kam es wieder zu erfolgreichen Angriffen mit Ransomware auf Organisationen im Gesundheitswesen:

- Anfangs Dezember wurde der US amerikanische Betreiber von Opioiden-Behandlungszentren «Behavioral Health Group» (BHG) Opfer eines Cyberangriffs[4]. BHG betreibt über 80 Klinken in 17 US-Bundesstaaten. Gemäss eigenen Angaben hat BHG temporär das IT-Netzwerk abgeschaltet, um zu verhindern, dass sich der Angriff weiter im Unternehmensnetzwerk ausbreitet. Medienberichten zu folge führte der Ausfall der IT-Systeme zu Problemen bei der Medikamentenausgabe. Zunächst war nicht bekannt, ob es sich um einen Ransomware Angriff handelt.

- Ende Dezember teilte die deutsche Compugroup Medical (CGM) mit, Opfer eines Ransomware Angriffes geworden zu sein[5]. CGM ist nach eigenen Angaben der marktführende Hersteller von Software für Arztpraxen, Labors und Kliniken. Gemäss Medienmitteilung des Unternehmens war die überwiegende Mehrheit der Kundensysteme nicht betroffen und weiterhin in Betrieb. Weitere Informationen und ob Lösegeld bezahlt wurden sind nicht bekannt.

- Daten des CyberPeace Institute[6] zeigen, dass in den letzte 18 Monate mindestens 39 Ransomware Gruppierungen Angriffe gegen Unternehmen im Sektor Gesundheit in über 27 Ländern gefahren haben. Für die meisten Angriffe auf solche Unternehmen war demnach «Conti», «Pysa» und «Hive» verantwortlich.

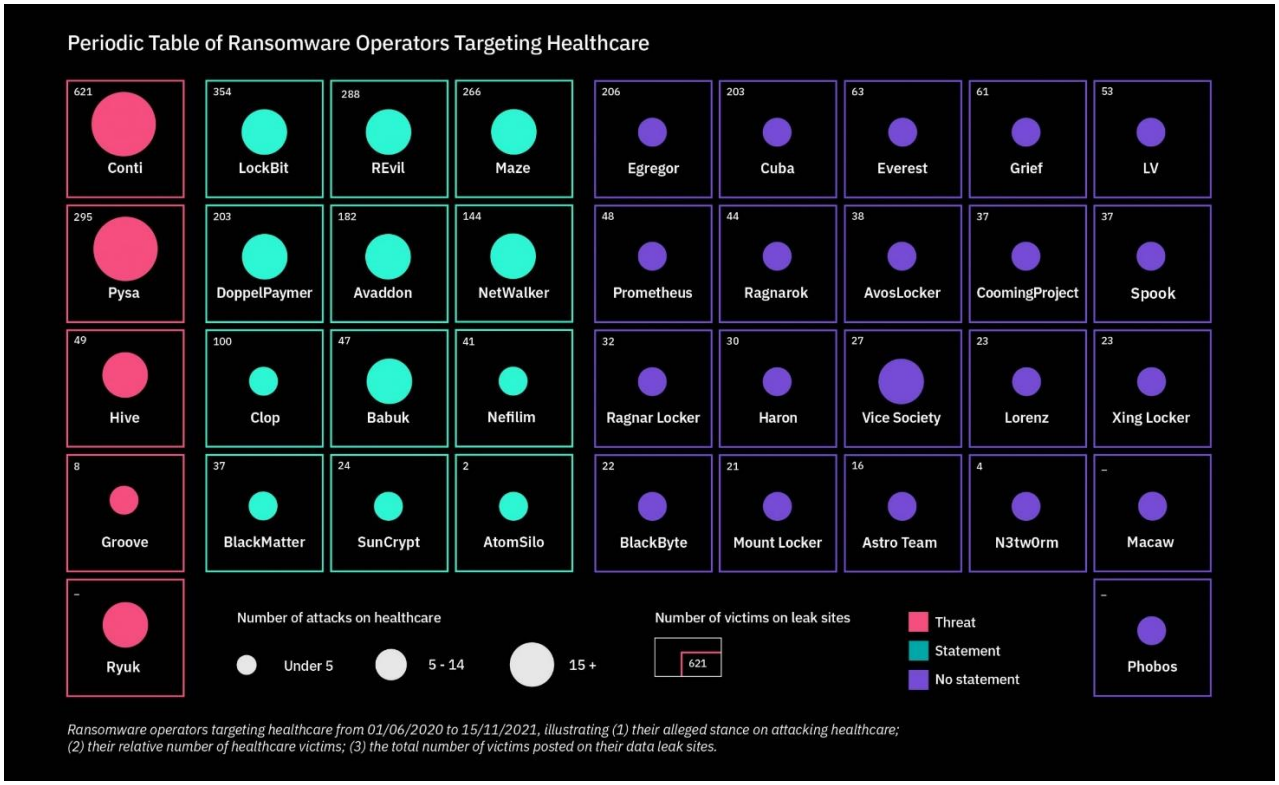

Figure 2 - Anzahl Ransomware Angriffe auf Sektor Gesundheit pro Ransomware Familie

[4] https://www.bleepingcomputer.com/news/security/cyberattack-on-bhg-opioid-treatment-network-disrupts-patient-care/

[5] https://www.cgm.com/corp_en/magazine/articles/emergency-note/technical-failure.html

[6] https://cyberpeaceinstitute.org/blog-series-reconceptualizing-ransomware/

In eigener Sache

Das «Cyber Security Update für Healthcare Sektor» wird ab 2022 neu vom Operation Information Center (OIC) vom Nachrichtendienst des Bundes (NDB) herausgegeben. Wir bedanken uns bei den Leser/innen für die Treue und hoffen, dass wir Sie auch in Zukunft zu unserer Leserschaft zählen können.

Ansprechpartner für technische Frage, Meldungen von Cyber-Vorfällen oder der Implementierung von Dienstleistungen des NCSC bleibt das GovCERT (siehe «Kontakt GovCERT»).

Empfehlungen:

- Gegen das Internet hin exponierte Systeme wie RDP, VPN Dienste, etc. müssen stets auf dem aktuellen Patch-Level gehalten werden. **Sicherheitsaktualisierungen müssen zeitnah eingespielt werden.**

- Administrationszugänge sollten nie ins Internet exponiert werden, sondern Beispielsweise nur über eine separate Netzzone («Management-Zone») zugänglich sein. Der Zugang auf eine solche Zone muss stark authentisiert (Zwei-Faktor-Authentisierung - 2FA) und sämtliche Zugriffe sollten aufgezeichnet werden. Geräte, welche für die Administration verwendet werden, sollten für keine anderen Zwecke gebraucht werden (insbesondere nicht für das Surfen im Web oder für E-Mails).

- **Remotezugänge** wie VPN und RDP sowie sämtliche andere Zugänge auf interne Ressourcen (z.B. Webmail, Sharepoint, etc) müssen zwingend mit einem zweiten Faktor abgesichert werden (**Zwei-Faktor-Authentisierung** – 2FA). Stellen Sie sicher, dass sie über einen genügend langen Zeitraum Logdaten aller erfolgreichen und fehlgeschlagenen Zugriffsversuchen haben. Speichern Sie diese Logdaten zentral und werten Sie diese regelmässig aus.

- Sperrung von IP-Adressen bekannter Botnetz Command&Control Server (C&Cs) durch Implementierung des **MELANI BGP Feeds** (Kontakt: outreach@govcert.ch). Ob Sie oder Ihr Provider diese bereits einsetzen, kann mit einem Aufruf der folgenden Test-Einträge mittels Web-Browser überprüft werden. Schlägt die Verbindung fehl, sind Sie bereits geschützt:
  - http://ip-protection.govcert.ch
  - http://melbl-protection.govcert.ch

- Sperren von Domain-Namen bekannter Botnetz Command&Control Server (C&Cs) durch Implementierung der **MELANI RPZ** oder des **Secure DNS Resolvers** für den Gesundheitssektor (Kontakt: outreach@govcert.ch)

- Blockieren Sie den Empfang von **gefährlichen E-Mail-Anhängen** auf Ihrem E-Mail-Gateway, dazu zählen auch **Office-Dokumente mit Makros**. Eine Empfehlung von zu sperrenden Dateianhängen finden Sie hier:
  - https://www.govcert.ch/downloads/blocked-filetypes.txt

- Erstellen **Sie regelmässig Sicherungskopien (Backups)** Ihrer Daten. Nutzen Sie dabei das Generationenprinzip (täglich, wöchentlich, monatlich - mindestens 2 Generationen, besser 3). Stellen Sie jeweils sicher, dass Sie das Medium, auf welchem Sie

die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer bzw. Netzwerk **physisch trennen und sicher aufbewahren**.

- Einsatz einer Liste wie URLHaus[7], um das Nachladen von Malware zu verhindern.
- Schützen und Überwachen sie zentrale Ressourcen wie ein Active Directory und bereiten Sie Notfallpläne für eine mögliche Kompromittierung vor.
- Nehmen Sie Meldungen von Behörden betreffend IT-Sicherheitsprobleme in Ihrem Unternehmen ernst. Bei Zweifel der Authentizität einer Meldung, fragen Sie telefonisch bei der Absenderbehörde nach.
- Stellen Sie sicher, dass Sicherheitsupdates zeitnah eingespielt werden. Hoch kritische Sicherheitsupdates müssen zudem sofort eingespielt und dürfen nicht auf das nächste Wartungsfenster verschoben werden.
- Wählen Sie Ihre Zulieferer (Supplier), insbesondere solche von IT-Dienstleistungen, sorgfältig aus und achten Sie darauf, dass Ihr Dienstleister «Best Practices» im Bezug zur Cybersicherheit ebenfalls umgesetzt hat. Stellen Sie vertraglich sicher, dass der Zulieferer Sie über relevante Cybervorfälle in seiner Firma sowie den möglichen Diebstahl von Kundendaten (Data breach) zeitnah informiert. Gewähren Sie Dienstleistern keine uneingeschränkten Remote Zugänge und sichern Sie diese soweit als möglich ab.

Kontakt GovCERT

Im Falle eines IT-Sicherheitsvorfalles, von verdächtigen E-Mails, etc. steht Ihnen das GovCERT jederzeit gerne zur Verfügung:

E-Mail: incidents@govcert.ch
Pikett-Telefon: +41 79 152 20 80 (**nur in Notfällen!**)

Für Rückfragen technischer Art oder Implementierung von GovCERT Dienstleistungen:
outreach@govcert.ch

[7] https://urlhaus.abuse.ch/